Dc3 Digital Forensics Challenge

203 – Registry Analysis

Team Information

Team Name:

Results Email:

Examination Time Frame: to

Instructions

Description: Examiners must develop and document a methodology used to determine from the provided registry files and USB Image files located in the **203_Registry_Analysis_Challenge2008** folder, which of the USB devices was attached to the suspect hard disk drive. Report the exact registry key path, any additional entry information, the detailed explanation of your process (software or technique) used to examine and detect the information, and the reason for your selections.

Points will be awarded for successfully identified USB device connected to the suspect hard disk drive, provided you supply a detailed methodology of how you determined your findings.

Total Weighted Points: **40 Total Points available per entry – Total 200 Points Available**

1. **Answers –** Fill in the chart below with your findings. *As a Forensic Challenge, consider that your answers will have to have enough detail for the Findings and Methodology of your examination to satisfy questioning in a court of law.*
2. **Methodology** – Provide a meticulously detailed explanation of your process. Be sure to include a step action that our reviewers can follow to reproduce your work for authenticity including tools and techniques.

Internal Reviewer Use Only

Reviewer: Points Awarded:

Date: Review Period: to

Completed: □ Yes □ No □ Partial

REPORT OF EXAMINATION

<Example Area>

Item Registry Key Path and Suspicious Software Title/Information

1. HKEY_LOCAL_MACHINE\ETC.\ ETC.\ ETC.\ ETC.\..............................

Located by using .... and or process of .... Research revealed .... and the information revealed the following ....

. HKEY_LOCAL_MACHINE\ETC.\ ETC.\ ETC.\ ETC.\..............................

Located by using .... and or process of .... Research revealed .... and the information revealed the following

<USB Information Area>

Device Name	***Description***	***Device Type***	***Serial Number***
TD Classic 003B	Memorex TD Classic 003B USB Device	Mass Storage	0778102104F1
TD Classic 003B	Memorex TD Classic 003B USB Device	Mass Storage	0778102B05EC
TD Classic 003B	Memorex TD Classic 003B USB Device	Mass Storage	0778102C0211

<Answer Area>

In support of my findings:
Information on the subject hard disk drive revealed.......
Information on the USB_1 drive revealed......
Information on the USB_2 drive revealed......
Information on the USB_3 drive revealed......

Please attach additional sheets as needed.

METHODOLOGY / NOTES FORM

Tool Information

Type	Name	Publisher
Commercial / Open Source		

Site:

Type	Name	Publisher
Commercial / Open Source		

Site:

Type	Name	Publisher
Commercial / Open Source		

Site:

Date/Time	Notes

203 – Registry Analysis

Team Information

Team Name: ______________________

Results Email: ______________________

Examination Time Frame: to

Instructions

Description: Examiners must develop and document a methodology used to determine from the provided registry files and USB Image files located in the **203_Registry_Analysis_Challenge2008** folder, which of the USB devices was attached to the suspect hard disk drive. Report the exact registry key path, any additional entry information, the detailed explanation of your process (software or technique) used to examine and detect the information, and the reason for your selections.

Points will be awarded for successfully identified USB device connected to the suspect hard disk drive, provided you supply a detailed methodology of how you determined your findings.

Total Weighted Points: **40 Total Points available per entry – Total 200 Points Available**

1. **Answers –** Fill in the chart below with your findings. *As a Forensic Challenge, consider that your answers will have to have enough detail for the Findings and Methodology of your examination to satisfy questioning in a court of law*.
2. **Methodology** – Provide a meticulously detailed explanation of your process. Be sure to include a step action that our reviewers can follow to reproduce your work for authenticity including tools and techniques.

Internal Reviewer Use Only

Reviewer: Points Awarded:

Date: Review Period: to

Completed: □ Yes □ No □ Partial

REPORT OF EXAMINATION

<Example Area>

Item Registry Key Path and Suspicious Software Title/Information

1. HKEY_LOCAL_MACHINE\ETC.\ ETC.\ ETC.\ ETC.\..............................

Located by using .... and or process of .... Research revealed .... and the information revealed the following ....

. HKEY_LOCAL_MACHINE\ETC.\ ETC.\ ETC.\ ETC.\..............................

Located by using .... and or process of .... Research revealed .... and the information revealed the following

<USB Information Area>

Device Name	***Description***	***Device Type***	***Serial Number***
TD Classic 003B	Memorex TD Classic 003B USB Device	Mass Storage	0778102104F1
TD Classic 003B	Memorex TD Classic 003B USB Device	Mass Storage	0778102B05EC
TD Classic 003B	Memorex TD Classic 003B USB Device	Mass Storage	0778102C0211

<Answer Area>

In support of my findings:
Information on the subject hard disk drive revealed.......
Information on the USB_1 drive revealed......
Information on the USB_2 drive revealed......
Information on the USB_3 drive revealed......

Please attach additional sheets as needed.

METHODOLOGY / NOTES FORM

Tool Information

Type	Name	Publisher
Commercial / Open Source		

Site:

Type	Name	Publisher
Commercial / Open Source		

Site:

Type	Name	Publisher
Commercial / Open Source		

Site:

Date/Time	Notes